NetEye

NetEye
User Group
2023

WÜRTHPHOENIX

Massimo Giaimo
Team Leader Cyber Security

Ransomware negotiation: dos and don'ts!

WÜRTHPHOENIX

Victim

In the ransom note,
you stated that you took 500 giga byte of information.
Our board is having issues with the quantifying the data.
To help them out, is there something I can hunt for to quantify this on the exfil side?
Based on this, then the board should be in a position to discuss options to satisfy your request of 8 millions dollars.

Gang

This is just business,
it makes no sense for us to lie or
not fulfill obligations.
If we do business this way,
there will be no profit for us.
We think that the provided data is
already enough to understand the seriousness
of your problem.
We have been in your network for more than
2 weeks and we think you understand that
there was enough time to download even more
information.
And also you will find out that
if we can't reach the agreement, then we will
have to publish some of the data in our blog.
You should also know that in 5 days the
amount will be doubled.

Victim

Thank you for providing this explanation. The board is asking for you to consider 800.000 dollars to find an agreement.
Can we agree to this amount?

Gang

Do you want us to give you a discount of more than 90%?
Of course this is impossible.
Apparently you do not realize the seriousness of the situation and the consequences.
Loss of reputation. Loss of clients and possible litigation with them.
Financial losses due to downtime.
Your data will also be seen by your competitors.
The stocks in the market will begin to fall, and this is clearly not to your investors' liking.
And much more. You are a big, serious company.
Be realistic. If you are ready to seriously discuss the deal in the near future, then we will be ready to slightly reduce the amount.
If your new proposal is again frivolous, we will have to prepare a blog post with the first part of the data.

NetEye

NetEye
User Group
2023

WÜRTHPHOENIX

Massimo Giaimo
Team Leader Cyber Security

Ransomware negotiation: dos and don'ts!

WÜRTHPHOENIX

Negotiation

is an interpersonal decision-making process that becomes necessary when it is not possible to achieve one's goals unilaterally.

The **negotiator** is the entity, for each party, who conducts the negotiation.

Negotiation

during a ransomware attack typically takes place in a restricted-access chat.

3 types of negotiation

- competitive
- cooperative
- integrative

Competitive N:

Ransomware Gang:
You have non chanches with $500,000 or this level of amounts of money, even don't try bluf by this. If you pay shortly, we accept $6,75M. If no, we start publication data part by part to speed up you.

- objective of obtaining an agreement that is advantageous for itself and disadvantageous for the other party:
- intimidate the opponent
- make him lose faith in his own negotiating skills
- force him to accept the agreement even if it is more disadvantageous than expected

Cooperative N:

Victim:
Okay, we understand how severe this is, and we will reach and agreement with you. In order for me to continue the conversation with our bosses here, can you send me a sample of stolen data from at least 2 different servers that are different than what was already posted to the website? Once we have that we will hopefully be able to quickly determine our budget and let you know how long it will take to save up the money.

- try to reach an agreement that is satisfactory for both parties
- we try to build a relationship with the other party, based on trust
- the negotiation must begin with concessions and proceed with moderate requests that are generally easily accepted by the opponent
- it works especially when both parties adopt it

Victim:
Leadership is taking you seriously and for now, they have approved a payment of $1,700,000 in an effort to move past this. We just don't know how long this money can stay on the table before we spend it elsewhere

Ransomware Gang:
According to your financial report your situation is much better than you say. As a group with an estimated yearly revenue $ 0,5 billion you have enough money to ay us. We are giving you one more discount and the price now is $8,000,000.

Integrative N:

- combines the 2 approaches
- both parties try to get as many concessions as possible from the other party
- as in the cooperative approach, the litigants attempt to reach an amicable settlement to the dispute

Negotiation. Why?

- At the beginning of an Incident Response process it is not clear what the ending might be.
- Why should I close all contact with the Threat Actor?
- What do I have to lose by contacting the Threat Actor?
- What if paying the ransom was the only viable choice to give your business a future?

Assumptions

- the ransom amount is not decided randomly
- Threat Actor:
  - don't like negotiators
  - **want** our money
  - **invest** money to attack
  - **need** our money

Dos (1/2)

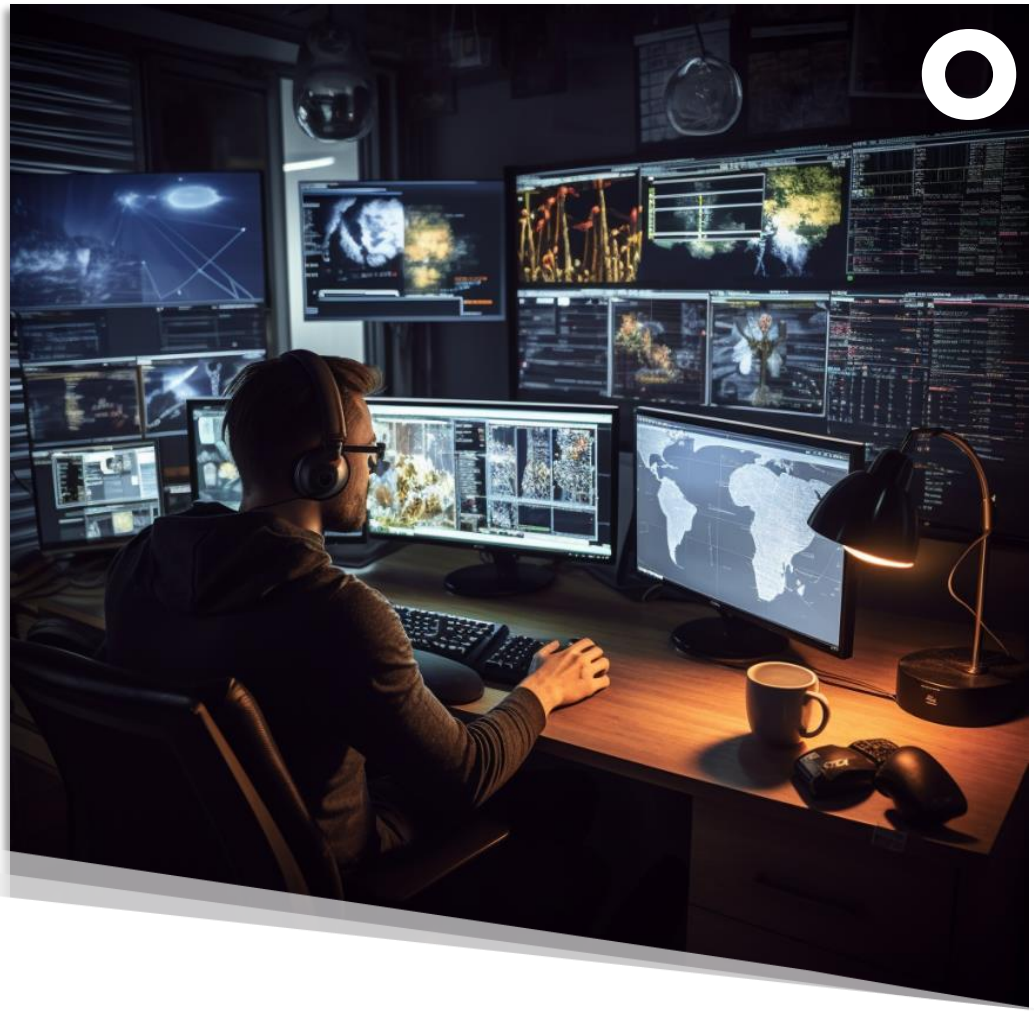
- calm and patience (which is the virtue of the strong!)
- maintain a professional and respectful tone
- show empathy towards the Threat Actor's situation and objectives
- make it clear to the other party that he is talking to the person who (or who is close to whom) can make decisions
- try to establish “tactical empathy” by mirroring the hacker’s language patterns

Dos (2/2)

- look for information on the gang that attacked your organization. You need to know the counterparty's reputation in order to best deal with it
- ask for proof of good functioning of the decryptor, both on small and large files
- make sure the negotiation chat is secure (AKA the private link has not been shared)
- prepares communications (precise, complete, transparent) for the various stakeholders

Don’ts

- don't try to fix the situation on your own. Involve relevant authorities and experts. Negotiation is not a theme to be improvised!
- do not share personal or confidential information with the gang. Just discuss the specific data and ransom situation.
- do not name any involvement of insurance companies
- do not threaten or provoke the Threat Actor. This could make the situation even more tense and damaging.



Our analysis

- #122 ransom chats
- #29 negotiation w payment
- #93 negotiation w/o payment

Aggressiveness index

I also negotiate in good faith, but I can't do it forever; my time is very expensive. When I see that negotiations are deadlocked and you do not hear me, there is no point in continuing negotiations. We are not in the Arab market to bargain here for 100-200 thousand dollars. You and I have serious businesses, we earn millions of dollars, the reputation of your business is priceless and can not be worth less than 5 million, if your leadership is adequate and understands that the business had to close, they will pay 5 million, it you are willing to close your business, enjoy your 5 million and do not pay me.

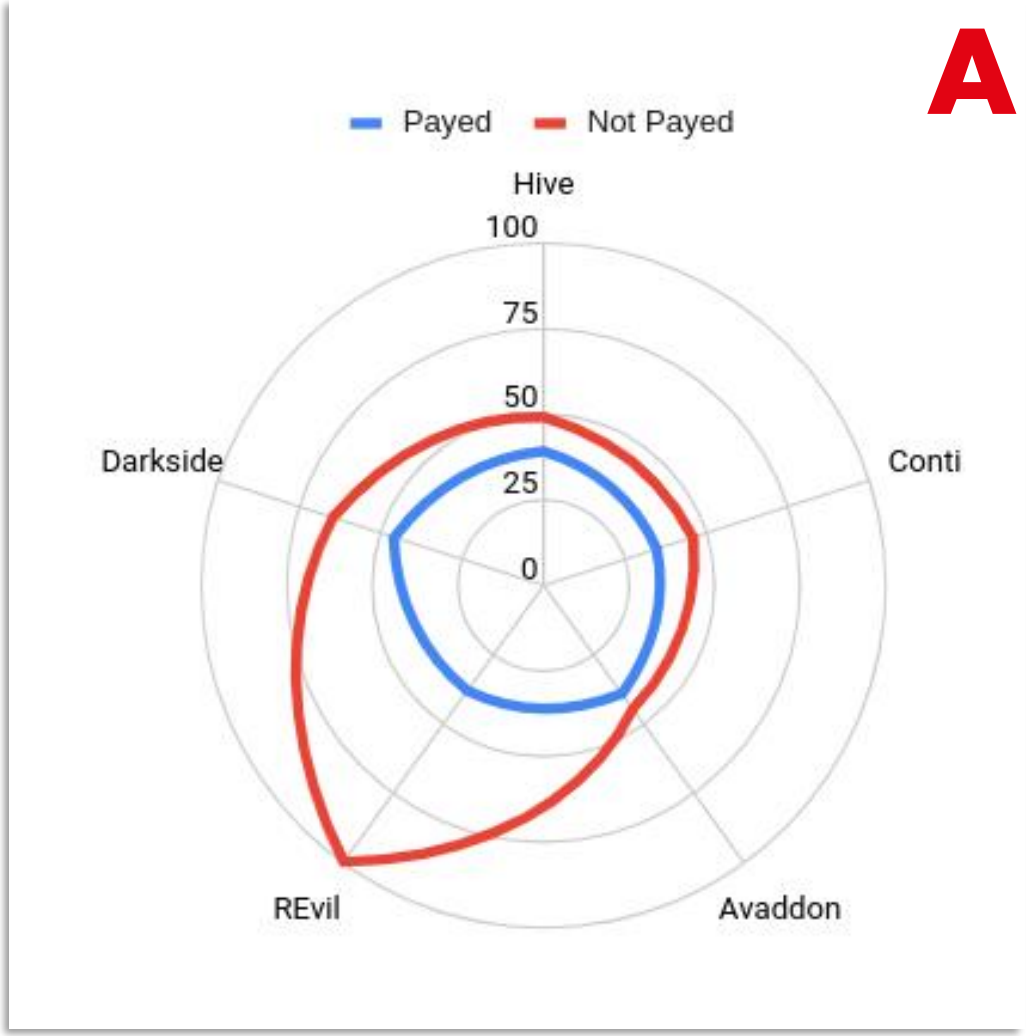
- Based on the words used in communications, we have drawn up 2 lists:
  - 1 of aggressive words
  - 1 of non-aggressive words
- We therefore calculated, for the Threat Actor and for the Victim, an aggressiveness index for the various communications.

Aggressiveness index

You know sir, current covid -19 pandemic really make all the human being life in difficulties. My first priority to save company data and my job. You're a unknown person, but I'm confident that you will help me to settle this problem. My pray will be with you. Kindly accept the offer and help me sir.

- Based on the words used in communications, we have drawn up 2 lists:
  - 1 of aggressive words
  - 1 of non-aggressive words
- We therefore calculated, for the Threat Actor and for the Victim, an aggressiveness index for the various communications.

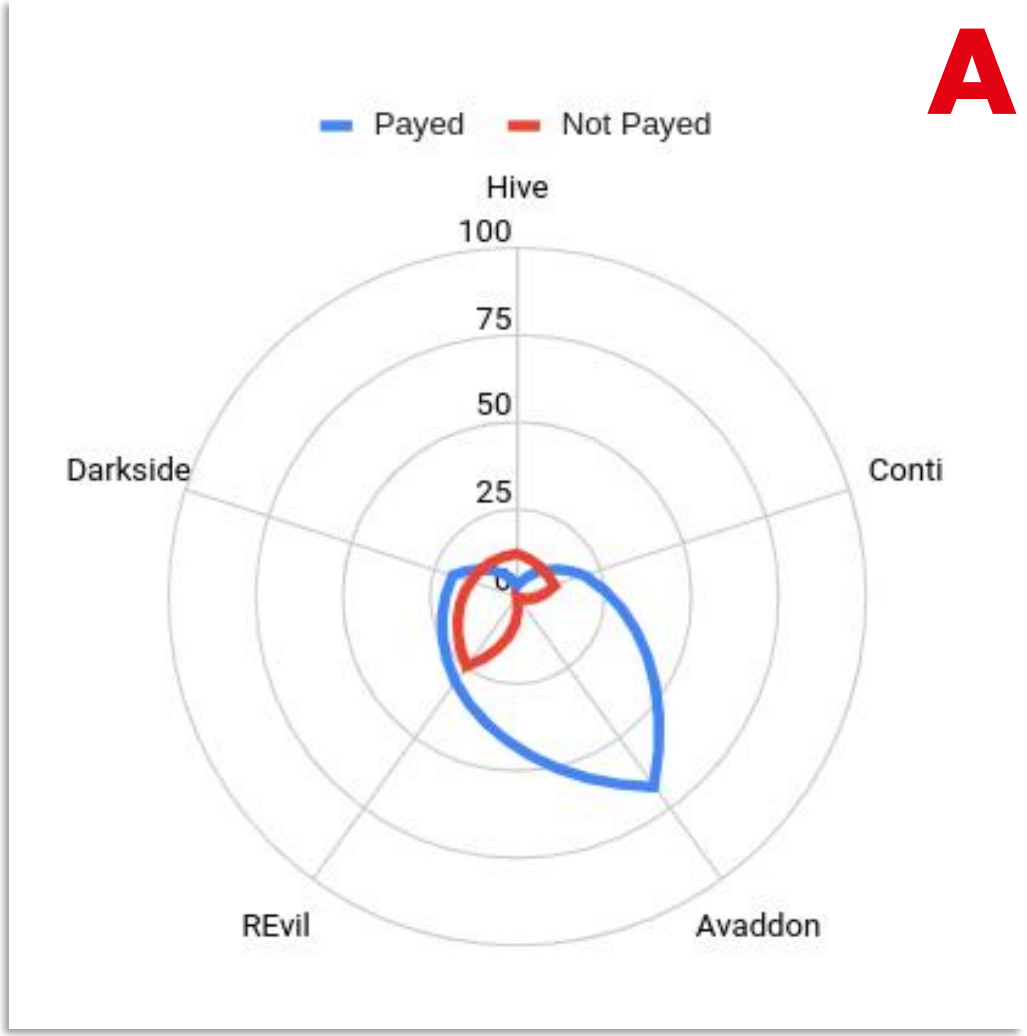
Aggressiveness index



Focus on gang

Gangs use more aggressive language when payment is not made.

Aggressiveness index



Focus on victims

Victims use more aggressive language when the payment occurs.

Negotation

Focus on Conti ransomware gang chats

Negotiation is a fundamental step, which allows you to increase the number of steps (and consequently the discount percentage on the initial request).

	Initial request	Paid	Discount %	Steps	AVG
	900.000,00	325.000,00	63,89	15	575.000,00
	1.500.000,00	350.000,00	76,67	10	1.150.000,00
	400.000,00	200.000,00	50,00	9	200.000,00
	1.700.000,00	120.000,00	92,94	8	1.580.000,00
	999.000,00	512.000,00	48,75	8	487.000,00
	980.000,00	300.000,00	69,39	7	680.000,00
	200.000,00	100.000,00	50,00	7	100.000,00
	5.000.000,00	746.500,00	85,07	6	4.253.500,00
	3.000.000,00	800.000,00	73,33	6	2.200.000,00
	900.000,00	450.000,00	50,00	6	450.000,00
	300.000,00	150.000,00	50,00	5	150.000,00
	150.000,00	100.000,00	33,33	3	50.000,00
	1.250.000,00	1.000.000,00	20,00	1	250.000,00
AVG	1.329.153,85	396.423,08	58,72	7	962.541,67

Read the full research @

https://www.neteye-blog.com/2023/09/ransomware-negotiation-dos-and-donts/

Thanks to Valéry Marchive (aka Casualtek) for Ransomchats project - https://github.com/Casualtek/Ransomchats

info@wuerth-phoenix.com
www.wuerth-phoenix.com

Thank you